PCT/JP01/06298
19.07.01

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　７月２４日

出願番号
Application Number: 特願２０００－２２２６８０

出願人
Applicant(s): 株式会社鷹山

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

２００１年　８月２４日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０７４７１８

【書類名】　特許願

【整理番号】　P00-0531

【提出日】　平成12年 7月24日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 9/36

【発明の名称】　電文送信装置及び電文受信装置

【請求項の数】　6

【発明者】

【住所又は居所】　東京都世田谷区北沢三丁目５番１８号　鷹山ビル　株式会社　鷹山内

【氏名】　高取　直

【発明者】

【住所又は居所】　東京都世田谷区北沢三丁目５番１８号　鷹山ビル　株式会社　鷹山内

【氏名】　清松　久典

【特許出願人】

【識別番号】　000127178

【氏名又は名称】　株式会社　鷹山

【代理人】

【識別番号】　100091096

【弁理士】

【氏名又は名称】　平木　祐輔

【選任した代理人】

【識別番号】　100105463

【弁理士】

【氏名又は名称】　関谷　三男

【選任した代理人】

【識別番号】　100110191

【弁理士】

【氏名又は名称】　中村　和男

【手数料の表示】

【予納台帳番号】　015244

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0002935

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電文送信装置及び電文受信装置

【特許請求の範囲】

【請求項１】　送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文をパケット通信方式で送信するデータ送信部と、を備えることを特徴とする電文送信装置。

【請求項２】　送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部と、前記電文順序並替部によって並べ替えられた送信電文及び前記制御電文生成部によって生成された制御電文をパケット通信方式で送信するデータ送信部と、を備えることを特徴とする電文送信装置。

【請求項３】　前記データ送信部は、前記電文順序並替部によって並べ替えられた送信電文と前記制御電文とを別に送信することを特徴とする請求項２記載の電文送信装置。

【請求項４】　前記ダミー電文は、前記送信電文の内容と異なる内容であって、送信電文の内容の把握を妨げる内容であることを特徴とする請求項１又は２記載の電文送信装置。

【請求項５】　パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した電文を記憶する受信電文記憶部と、該受信電文記憶部に記憶されている電文からダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備えることを特徴とする電文受信装置。

【請求項６】　パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した受信電文を記憶する受信電文記憶部と、該データ受信部で受信した制御電文を記憶する制御電文記憶部と、前記受信電文記憶部に記憶されている電文から前記制御電文記憶部に記憶されている制御電文に基づいてダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備え

ることを特徴とする電文受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、送信電文及びダミー電文を分割しかつそれらの順序を入れ替えて伝送することで、盗聴等による電文内容の把握を困難にした電文送信装置及び電文受信装置に関する。

【０００２】

【従来の技術】

インターネットの普及により個人情報などの機密性の高い情報を電子メール等により送信する機会が増えている。インターネットはある情報を送る場合、そのデータをまずパケットに分割する。これら各パケットにはヘッダといわれる標識が付き、このヘッダに行き先やパケットを再度組み立てるときの順番などの情報が記されている。このヘッダのあるおかげで、たとえどこかの回線が断たれたとしても各パケットはいくつかの違う順路をたどって目的地に着くことができ、そこで元の通りに再構築され、正確な情報に再現される。この方式だと、１つの回線上をいくつもの行き先の異なったパケットが通過できるので、効率がきわめて良く、データ通信には優れた方式だといえる。

【０００３】

インターネットは各地域や学校・企業などの単位がもつネットワーク同士がつながっており、そのつなぎ目にあたるところにはルーターと呼ばれるコンピュータが介在する。ルーターは到着してくるパケットのヘッダを読み取って目的地へと再び送り出し、そのようなことが繰り返されてパケットは最終目的地にたどり着く。このようにデータ（情報）はインターネットにつながれたネットワークのルーターをリレー式に送られながら目的地にたどり着くので、このような情報伝達方式を称して「バケツリレー式」などといったりする。

【０００４】

パケット通信によっていくつもの中継地点を通過するため、その間でデータを盗聴される危険がある。そこで、データを安全に送受信するために、各種の暗号

方式が実用化されている。送信側で平文を解読が困難な暗号文に暗号化し、受信側で暗号文を平文に復号化するには多くのデータ処理が必要があり、暗号化／復号化のためのプログラムや送受信装置の構成が複雑になるとともに、処理能力の高いプロセッサが必要になることがある。

【０００５】

特開平９－１８４７３号公報には、ユーザデータ全てを暗号化して伝送するような高い処理能力を持たないプロセッサを使用して、単純な手法によりユーザデータを秘匿してデータ通信を行えるようにしたデータ伝送装置が記載されている。このデータ伝送装置は次のように構成されている。送信が要求されたユーザデータをサブユーザデータに分割し、送信するパケットデータ内で分割したサブユーザデータをランダムに再配置し、さらに、送信するパケットデータを故意にランダムな順序に並べ替える。そして、パケットデータ中の通信制御情報（ユーザデータ順序番号や送達確認情報や再送情報等）の固定長のデータを暗号化して送信する。受信側では、通信制御情報を復号化し、その中に含まれているユーザデータ順序番号に係るキー情報に基づいてユーザデータを復元する。

【０００６】

また、特許公開２０００－１２４８９１号公報には、暗号化された暗号化データとその暗号化のために用いられた暗号化方式とを同時に送信せずに、別個独立に時間差をもって送信することで、安全性の向上を期待するようにしたデータ送受信装置が記載されている。

【０００７】

【発明が解決しようとする課題】

しかしながら、上記特開平９－１８４７３号公報に記載されているデータ伝送装置においても通信制御情報を暗号化／復号化する必要があり、通信制御情報を暗号化／復号化するために多くのデータ処理が必要である。

本発明はこのような課題を解決するためなされたもので、簡易なデータ処理で第三者による電文内容の把握を困難にした電文送信装置及び電文受信装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】

本発明の電文送信装置は、送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文をパケット通信方式で送信するデータ送信部と、を備える。

【０００９】

また、本発明の電文送信装置は、送信電文及びダミー電文を複数の電文にパケット単位で分割する電文分割部と、該電文分割部によって分割された電文の順序を並べ替える電文順序並替部と、該電文順序並替部によって並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部と、前記電文順序並替部によって並べ替えられた送信電文及び前記制御電文生成部によって生成された制御電文をパケット通信方式で送信するデータ送信部と、を備える。

【００１０】

また、前記データ送信部は、前記電文順序並替部によって並べ替えられた送信電文と前記制御電文とを別に送信することで、第三者による電文解読をより困難なものにすることができる。

また、前記ダミー電文は、前記送信電文の内容と異なる内容であって、送信電文の内容の把握を妨げる内容であることで、送信電文の内容の把握をより困難なものにできる。

【００１１】

また、本発明の電文受信装置は、パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した電文を記憶する受信電文記憶部と、該受信電文記憶部に記憶されている電文からダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備える。

【００１２】

また、本発明の電文受信装置は、パケット通信方式でデータを受信するデータ受信部と、該データ受信部で受信した受信電文を記憶する受信電文記憶部と、該データ受信部で受信した制御電文を記憶する制御電文記憶部と、前記受信電文記

憶部に記憶されている電文から前記制御電文記憶部に記憶されている制御電文に基づいてダミー電文を除去してパケット単位で並べ替えて電文を復元する電文復元部と、を備える。

【００１３】

【発明の実施の形態】

以下、添付図面を参照しながら本発明の好適な実施の形態について詳細に説明する。

図１は、本発明に係る電文送信装置及び電文受信装置のブロック構成図である。電文送信装置１０は、送信電文を複数の電文に分割する送信電文分割部１１と、ダミー電文を複数の電文に分割するダミー電文分割部１２と、分割された送信電文及び分割されたダミー電文の順序を並べ替える電文順序並替部１３と、並べ替えられた送信電文を元の順序に戻すための制御情報を有する制御電文を生成する制御電文生成部１４と、並べ替えられた各分割電文及び制御電文をそれぞれパケット通信方式で送信するデータ送信部１５とからなる。

【００１４】

電文受信装置２０は、データ受信部２１と、受信した分割電文を一時記憶する受信電文記憶部２２と、受信した制御電文を一時記憶する制御電文記憶部２３と、制御電文に含まれている制御情報に基づいて並べ替えられた電文を元の順序に戻して電文を復元する電文復元部２４とからなる。

電文送信装置１０と電文受信装置２０とはインターネット３０等のオープンなネットワークを介して接続される。

【００１５】

図２は、送信電文分割部及びダミー電文分割部の動作を示す図である。ここでは送信電文及びダミー電文をそれぞれ８個の電文に分割する例を示している。送信電文分割部１１は、図２（ａ）に示す送信電文Ｓを、図２（ｂ）に示すように８個の電文Ｓ１～Ｓ８に分割する。ダミー電文分割部１２は、図２（ｃ）に示すダミー電文Ｄを、図２（ｄ）に示すように８個の電文Ｄ１～Ｄ８に分割する。なお、分割するバイト数は任意であり、各分割部毎にそのバイト数が異なっていてもよい。

【００１６】

図３は、電文順序並替部の動作を示す図である。電文順序並替部１３は、図３（ａ）に示すように、分割された各電文Ｓ１～Ｓ８，Ｄ１～Ｄ８をその番号順に一時記憶する。電文順序並替部１３は、分割された電文の総数を認識する。ここでは、分割された電文の総数が１６であることを認識する。電文順序並替部１３は、分割された電文の総数の範囲で乱数を順次発生し、発生した乱数に基づいて電文順序の並べ替えを行う。なお、電文順序並替部１３は、複数の並べ替え順序を予め備えており、その中からランダムに１つの並べ替え順序を抽出し、抽出した並べ替え順序に基づいて電文順序の並べ替えを行うようにしてもよい。電文順序の並べ替え結果の一例を図３（ｂ）に示す。

【００１７】

図４は、制御情報の例を示す図である。制御電文生成部１４は、電文順序の並べ替えの結果に基づいて並べ替えられた電文を元の順序に戻すための制御情報を生成する。図４（ａ）に示す制御情報は、並べ替えられた電文の順序を示すようにしたもので、０はダミー電文であることを、１～８は送信電文であることを示している。ここで、図４（ａ）は最初がダミー電文、２番目が分割された送信電文の７番目、３番目がダミー電文、４番目がダミー電文、５番目が分割された送信電文の５番目、……、最後が送信電文の６番目であることを示している。

【００１８】

図４（ｂ）に示す他の制御情報は、分割された送信電文の１番目（Ｓ１）が１２番目のパケットで送信され、分割された送信電文の２番目（Ｓ２）が７番目のパケットで送信され、分割された送信電文の３番目が９番目のパケットで送信され、……、分割された送信電文の８番目が１０番目のパケットで送信されることを示している。

なお、図４では、カンマ区切りの文字列からなる制御情報を例示したが、区切り記号は例えばスペース文字や／，＊，＋等の記号文字等の任意に記号を用いることができる。

【００１９】

図５は、データ送信部の動作を示す図である。データ送信部１５は、図３（ｂ

）に示した並べ替え後の電文のそれぞれについてインターネットのプロトコルに対応したパケットにして、生成したパケットを順次送信する。具体的には、分割された電文（電文データ）の前にＴＣＰヘッダを付加し、さらにＴＣＰヘッダの前にＩＰヘッダを付加し、さらにその前にデータリンク層のヘッダを付加して送信する。ここで、データ送信部１５は、最初の電文Ｄ４を送信するパケットに対しては、ＴＣＰヘッダ内のシーケンスナンバー（何番目のパケットかを示す通し番号）を１とし、２番目の電文Ｓ７を送信するパケットに対しては、ＴＣＰヘッダ内のシーケンスナンバーを２とし、それ以降の各パケットに対して３，４，５，……のシーケンスナンバーをそれぞれ付けて送信する。また、データ送信部１５は、ＩＰヘッダ内の送信元ＩＰアドレスに本電文送信装置１０（電文送信側のコンピュータ）のＩＰアドレスを、ＩＰヘッダ内の宛先（送信先）ＩＰアドレスに送信先（電文受信装置２０を備える電文受信側のコンピュータ）のＩＰアドレスを付ける。

【００２０】

データ送信部１５は、分割された電文を全てパケット化して送信した後に、その通信を終了させる。そして、その後に電文受信装置２０との通信を再度開始する要求を発生し、制御電文生成部１４で生成した制御電文をパケット化して送信する。なお、データ送信部１５は、分割された電文を全てパケット化して送信した直後に、その通信を終了させることなく、制御電文をパケット化して送信するようにしてもよい。

【００２１】

なお、データ送信部１５とデータ受信部２１との間では、パケットの到着確認処理やパケットが正常に到着できなかったときの再送信処理等がなされる。なお、これらの処理等はＴＣＰプロトコル及びＩＰプロトコルで規定されている。

【００２２】

電文受信装置２０側のデータ受信部２１は、受信したパケットが電文パケットである場合は、その電文パケット中の電文を受信電文記憶部２２へ供給し、受信したパケットが制御パケットである場合は、その制御パケット中の制御情報（制御電文）を制御電文記憶部２３へ供給する。

【００２３】

なお、データ受信部２１は受信したパケットのデータに基づいて電文であるか制御情報であるかを判断するようにしている。具体的には、受信したデータが区切り文字等で区切られたデータである場合は制御情報と判断し、それ以外は電文であると判断する。なお、複数のパケットから構成されている場合には電文であると判断し、単一のパケットのみである場合には制御情報と判断するようにしてもよい。また、データ送信部１５側でＴＣＰヘッダ内に電文と制御情報とを区別する情報を挿入して送信し、データ受信部２１はＴＣＰヘッダ内に挿入された情報に基づいて電文と制御情報とを判別するようにしてもよい。また、データ送信部１５側で制御パケットを送信する際には、データ部に制御情報であることを示す情報を挿入しておき、データ受信部２１はデータ部内に制御情報であることを示す情報が挿入されているか否かに基づいて電文であるか制御情報であるかを判断するようにしてもよい。

【００２４】

受信した電文データは、そのパケットのシーケンスナンバー（何番目のパケットかを示す通し番号）との対応を付けて受信電文記憶部２２に一時記憶される。また、受信した制御情報は制御電文記憶部２３に一時記憶される。

【００２５】

図６は、電文復元部の動作を示す図である。電文復元部２４は、制御電文記憶部２３に記憶された制御情報に基づいて受信電文記憶部２２に記憶された電文を抽出して受信電文を復元する。具体的には、図６（ａ）に示す受信電文記憶部２２に記憶された電文の中から制御情報に基づいて分割された電文の第１番目を取り出し、次に分割された電文の第２番目，第３番目，……を順次取り出し、取り出した順に各電文を連結することで、図６（ｂ）に示すように、分割される前の電文（送信電文）を復元する。

【００２６】

本発明に係る電文送信装置は、電文を分割しその順序を並べ替えているだけであるので、インターネット３０上を伝送されるデータは断片化されているとはいえ平文である。しかしながら、有意な送信電文とダミー電文とが混在されて断片

化されているので、インターネット３０上を伝送されるデータを盗聴したとしたも、送信電文の内容を把握することは困難である。さらに、ダミー電文の内容を工夫することで、送信電文の内容把握をさらに困難にすることができる。例えば、本来の送信電文の内容が例えば「甲案に賛成」であった場合、ダミー電文の内容を「乙案に賛成」としたり、「甲案に反対」としたりすることで、第三者による内容の把握をさらに困難にすることができる。なお、ダミー電文は送信者が自ら作成してもよいし、コンピュータを利用してダミー電文を自動的に生成するようにしてもよい。

【００２７】

図１では、電文送信装置１０側で分割した電文をランダムに並べ替え、その並べ替え順序に関する制御情報を制御電文（制御パケット）として送信する構成を示したが、送信側と受信側とで予め並べ替える順序を定めている場合は、制御電文（制御パケット）の送受は不要となる。この場合は、制御電文生成部１４及び制御電文記憶部２３を設ける必要がない。

【００２８】

本発明では、制御パケットを開かない限り分割された電文を復元する順序を確定できない。したがって、制御パケットの経路履歴や開封確認をチェックすれば、送信内容を第三者に正確に把握されることを防止できる。そこで、制御パケットが各ルータを通過する際に、そのルータを特定するための情報（例えばルータのＵＲＬ）が制御パケットに追加記録されるようにすることで、制御パケットがどのような経路を経て受信側へ到達したかの経路ログを得ることができる。さらに、制御パケットが開封された際に開封された旨の情報が制御パケットに記録され、制御パケットが複製された際に複製された旨の情報が制御パケットに記録されるようにすることで、制御パケットを受信した時点で何らかの不正アクセスがあったか否かを特定することが可能となる。そして、電文受信装置２０は、途中で開封された旨の記録があるパケットを受信した場合には、その旨を電文送信装置１０側に通知し、受信電文を廃棄することで正常でない電文を復元するおそれをなくすことができる。

【００２９】

【発明の効果】

以上説明したように本発明は、送信側において送信電文及びダミー電文を分割しそれらの順序を並べ替えて送信するので、断片化されかつダミーの電文が含まれているため、電文が盗聴等された場合でも電文内容を正確に把握するのが困難である。本発明は、共通鍵方式や公開鍵方式等の暗号化処理／復号化処理を一切用いていないので、送信側及び受信側の構成及びデータ処理を簡易なものにすることができる。

【図面の簡単な説明】

【図１】

本発明に係る電文送信装置及び電文受信装置のブロック構成図である。

【図２】

送信電文分割部及びダミー電文分割部の動作を示す図である。

【図３】

電文順序並替部の動作を示す図である。

【図４】

制御情報の例を示す図である。

【図５】

データ送信部の動作を示す図である。

【図６】

電文復元部の動作を示す図である。

【符号の説明】

１０　電文送信装置

１１　送信電文分割部

１２　ダミー電文分割部

１３　電文順序並替部

１４　制御電文生成部

１５　データ送信部

２０　電文受信装置

２１　データ受信部

２２　受信電文記憶部

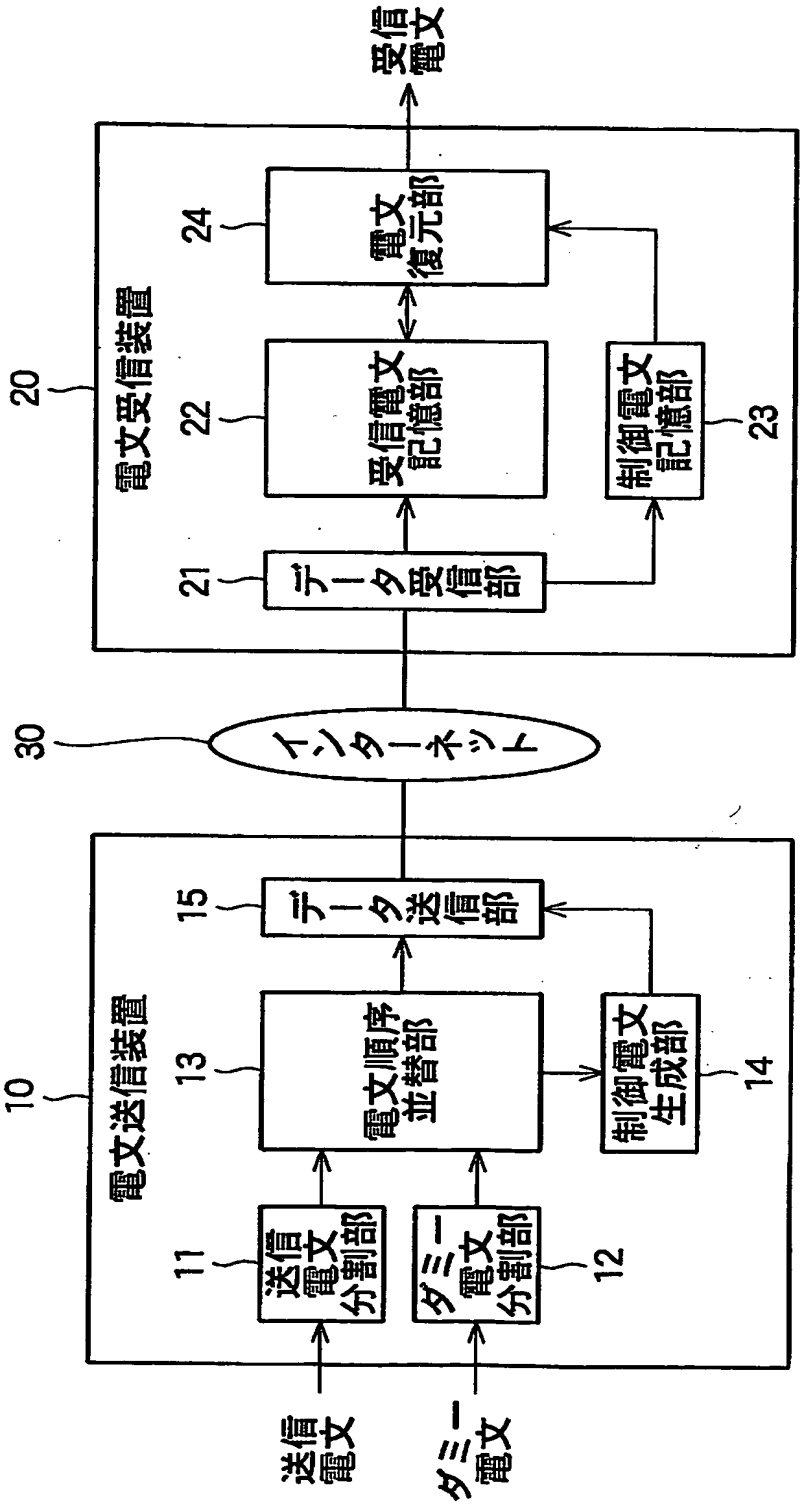
２３　制御電文記憶部

２４　電文復元部

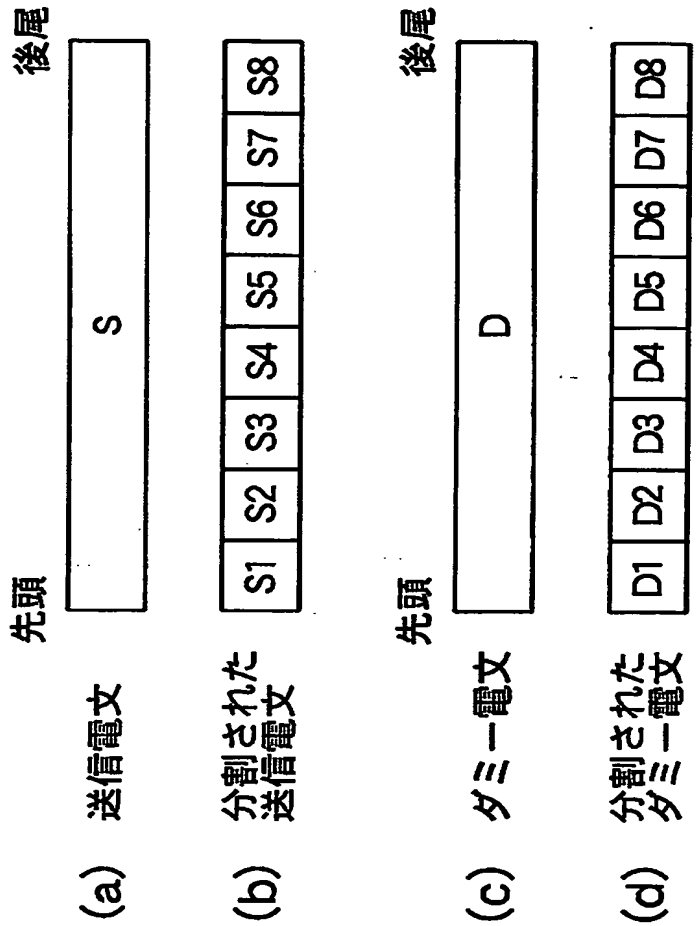
３０　インターネット

【書類名】　　図面

【図１】

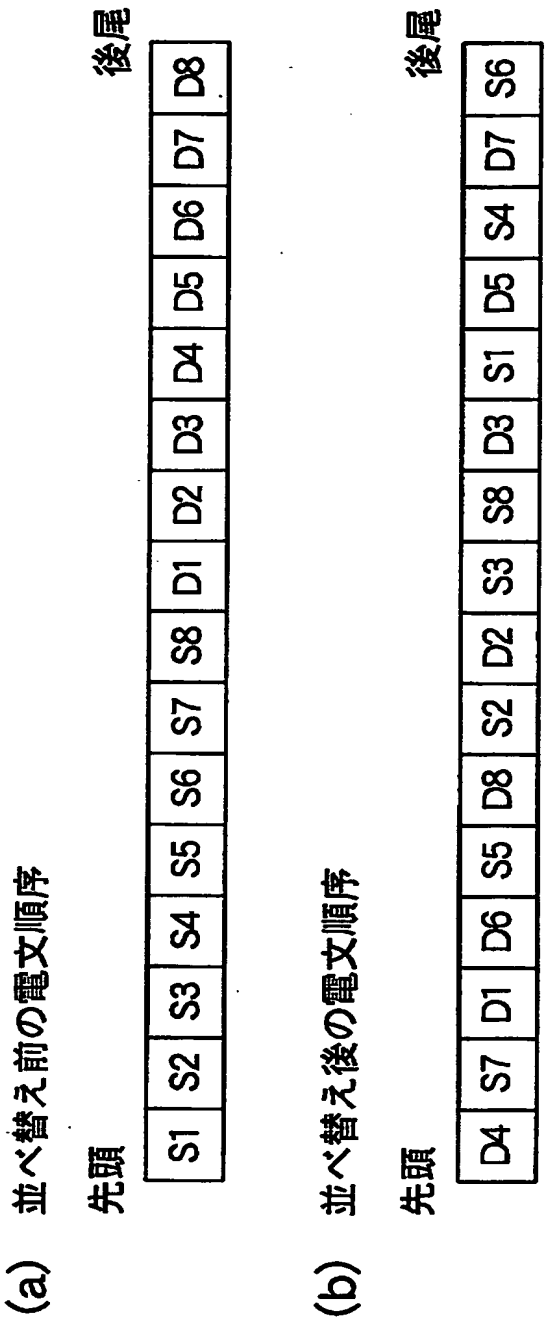

受信電文
電文受信装置
20
24
電文復元部
22
受信電文記憶部
23
制御電文記憶部
21
データ受信部
30
インターネット
電文送信装置
10
15
データ送信部
13
電文順序並替部
14
制御電文生成部
11
送信電文分割部
12
ダミー電文分割部
送信電文
ダミー電文

【図２】



出証特２００１－３０７４７１８

【図３】


(a) 並べ替え前の電文順序
先頭
後尾
S1 S2 S3 S4 S5 S6 S7 S8 D1 D2 D3 D4 D5 D6 D7 D8
(b) 並べ替え後の電文順序
先頭
後尾
D4 S7 D1 D6 S5 D8 S2 D2 S3 S8 D3 S1 D5 S4 D7 S6

【図４】

(a) 制御情報(一例)

先頭　　後尾

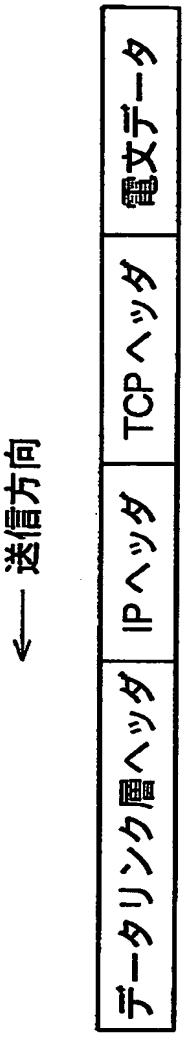
0, 7, 0, 0, 5, 0, 2, 0, 3, 8, 0, 1, 0, 4, 0, 6

(b) 制御情報(他の例)

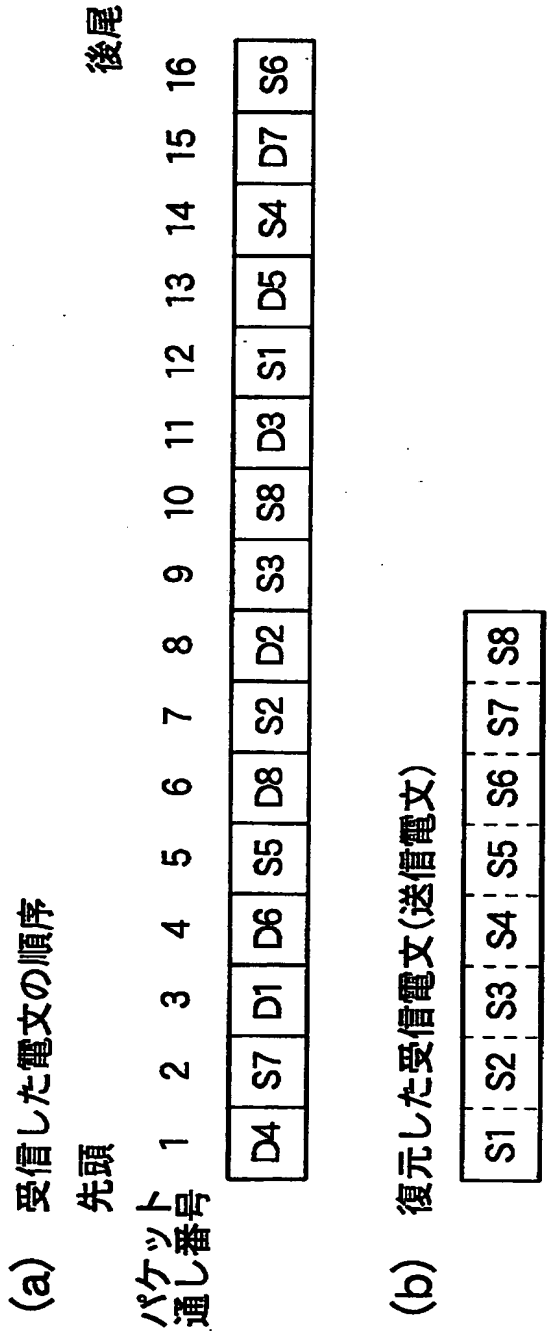
先頭　　後尾

12, 7, 9, 14, 5, 16, 2, 10

【図５】



【図６】


(a) 受信した電文の順序
先頭
後尾
パケット通し番号
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
D4 S7 D1 D6 S5 D8 S2 D2 S3 S8 D3 S1 D5 S4 D7 S6
(b) 復元した受信電文(送信電文)
S1 S2 S3 S4 S5 S6 S7 S8

【書類名】　要約書

【要約】

【課題】　送信電文及びダミー電文をそれぞれ分割して混合しかつそれらの順序を入れ替えて伝送することで、盗聴等による電文内容の把握を困難にする。

【解決手段】　電文送信装置１０は、送信電文を送信電文分割部１１で分割し、ダミー電文をダミー電文分割部１２で分割し、分割した各電文の順序を電文順序並替部１３で並べ替える。制御電文生成部１４は、並べ替えられた送信電文を元の順序に戻すための制御情報からなる制御電文を生成する。データ送信部１５は、並べ替えられた送信電文を１つ毎にパケット化し、パケット通し番号を付けて送信する。データ送信部１５は、送信電文とは別途に制御電文をパケット化して送信する。電文受信装置２０は、受信した電文をパケット通し番号との対応を付けて受信電文記憶部２２に格納する。電文復元部２４は、受信した制御情報に基づいて電文の順序を元に戻して連結することで、本来の送信電文を復元する。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　　〔０００１２７１７８〕

１．変更年月日　　１９９８年１１月１６日
［変更理由］　名称変更
住　所　東京都世田谷区北沢３－５－１８
氏　名　株式会社鷹山